Sniffer Portable

The best-in-class, plug-and-play network and application analyzer

Highlights

- Faster time-to-knowledge for network and application problems
- Dashboard views with deep drill-down to rich packet-level analysis
- Wired and wireless support in a single, scalable tool
- Best-in-class network and application analysis functionality

Sniffer® Portable Professional network analyzer is a best-in-class, plug-and-play, single-user analyzer for network and application troubleshooting. Sniffer Portable Professional gives network managers on-demand monitoring, packet capture and problem analysis for wired and wireless network segments. Ideal for rapid response to network and application issues on location in the field, the software-based solution offers powerful troubleshooting tools at a cost-effective price point.

Built on the industry's most advanced and widely-deployed Sniffer network analyzer software, Sniffer Portable Professional provides best-of-breed network and application performance troubleshooting. A wide range of protocol decodes are supported for both on-demand and post-capture analysis, including popular VoIP, wireless, financial and mobile protocols. Rich expert modes assist users in quickly identifying errors during packet-level analysis. Sniffer Portable Professional delivers intuitive, easy-to-use dashboards and network views that include deep packet drill-down capabilities and support for wired 10/100/1000 Ethernet and wireless 802.11 a/b/g/n networks all in one tool - yielding consistent operation and functionality, reducing desktop tool clutter and greatly accelerating problem resolution.

Sniffer Portable Professional can be used to:

- Rapidly identify network and application performance issues over wired and wireless networks
- Troubleshoot new technologies, applications or services deployments - in production and prior to rollout
- Monitor and validate infrastructure changes
- Analyze and validate security threats on wired and wireless network links as well as the wireless control infrastructure

On-Demand Monitoring

Sniffer Portable Professional provides a detailed analysis of network traffic and application performance using its dashboard view, and drill-downs into deep packet inspection. The dashboard displays important data about the network. It creates statistical measurements about network traffic, providing an accurate picture of network activity in real time. Network managers can easily drill down from the dashboard to view individual hosts and protocols.

Within the Sniffer Portable Professional dashboard network, engineers can monitor both network and application statistics, including:

Network statistics

- Number of packets and bytes
- Percentage of utilization
- Broadcast and multicast counts
- Packet size distribution statistics
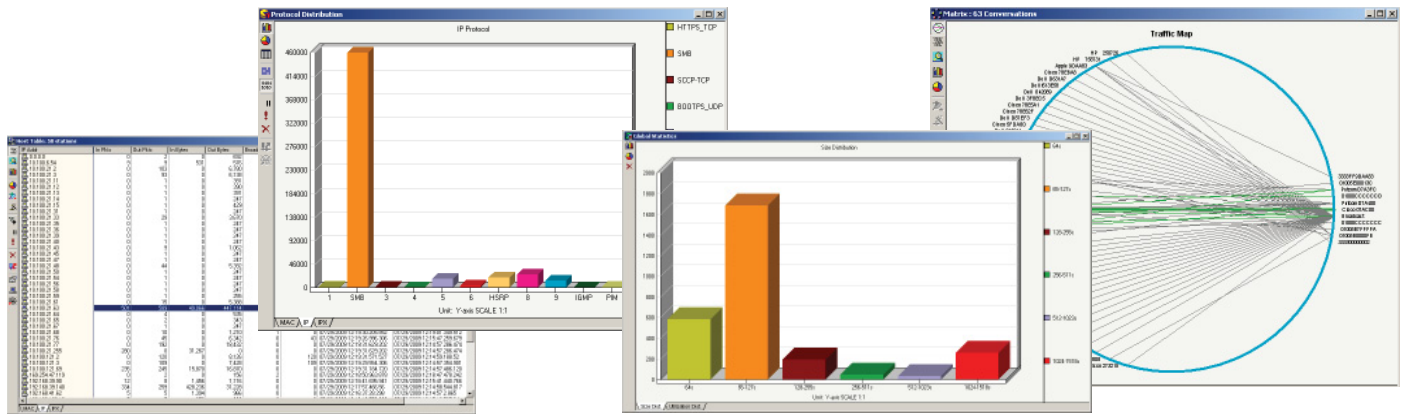- Network error statistics
- Protocol usage statistics

Figure 1: Sniffer Portable Professional analyzer provides best-in-class analyzer functionality with on-demand packet capture, Expert analysis and robust decodes for wired and wireless subnets.

Application statistics

• Individual hosts and conversation-pair traffic statistics

• Top talkers, top applications

• Response time statistics

• Applications in use per user

• Show fastest/slowest server-client pair

Packet Capture, Decodes, Expert Analysis

The Sniffer Portable Professional capture function collects and stores the actual packets traversing the network segment in question. During capture, Expert analysis is performed on packets and results are displayed in an easy-to-read, real-time view.

On-Demand and Post-Capture Decodes

Sniffer Portable Professional displays protocol decodes in real-time and decodes application and technology protocols as the packets are captured. Advanced filtering options are available for drilling down on particular conversations based on IP address or port number. The decode view provides classic, line-by-line protocol interpretation of the network data. When real-time contents or content from a capture file is displayed, Sniffer Portable Professional interprets and decodes the protocol. The decode view shows the results of this protocol analysis, displaying packets in three color-coded viewing panes: summary, detail, and hex codes. Capture files are stored short-term, providing a snapshot in time for troubleshooting.

On-Demand Expert Analysis

Sniffer Portable Professional analyzes network packets during or post capture and uses this information to create alerts for potential problems on the network. These problems are categorized as either symptoms and/or diagnoses. During Expert analysis, a database of network objects is constructed from the traffic seen. Sniffer Portable Professional learns all about the network stations, routing nodes, sub networks, and connections related to the packets in the capture buffer and uses this information to alert users to potential issues.

Focused Filters and Triggers

Sniffer Portable Professional gives network managers the ability to create filters for the particular traffic needed for network analysis in order to isolate and quickly identify network problems. Filters provide a way to narrow in on the precisely data needed to troubleshoot a network problem. Filters also help reduce the size of files collected for historical records. Triggers can be set to start captures at specific times, or in response to specific events, such as on off-hours or weekends.

Alarms and Notifications

Alarm features provide a comprehensive method of detecting and logging network alarm events. Expert analysis can generate alarms during data capture and log an event in the alarm log when it detects a symptom or diagnosis. Upon startup, Sniffer Portable Professional logs events in the alarm log when a user-specified threshold parameter is exceeded.

Abnormal network events can be assigned to one of five different levels of severity: Critical, Major, Minor, Warning, and Informational. In addition, severity levels can be associated with up to four alarm notification actions. For example, Sniffer Portable Professional can trigger an alarm and an action can be activated to initiate a packet capture.

Wireless Capabilities

Sniffer Portable Professional provides two connectivity options for performing wireless network analysis:

1. Connected to a wired switch span port via Ethernet, Sniffer Portable Professional uses the laptop wireless card in promiscuous mode to monitor wireless traffic from devices within range

2. Connected to a wireless access point via one laptop wireless card, Sniffer Portable Professional uses a second laptop wireless card in promiscuous mode to monitor wireless traffic from devices within range

Wi-Fi Device List

Sniffer Portable Professional provides an inventory of all 802.11a, 11b, 11g and 11n devices operating in the wireless environment. It provides detailed information on the configuration settings that are available or are in use on the devices, including critical parameters such as signal strength, noise, SSID, security settings in use, associated devices, cell power, device activity status, and many more.
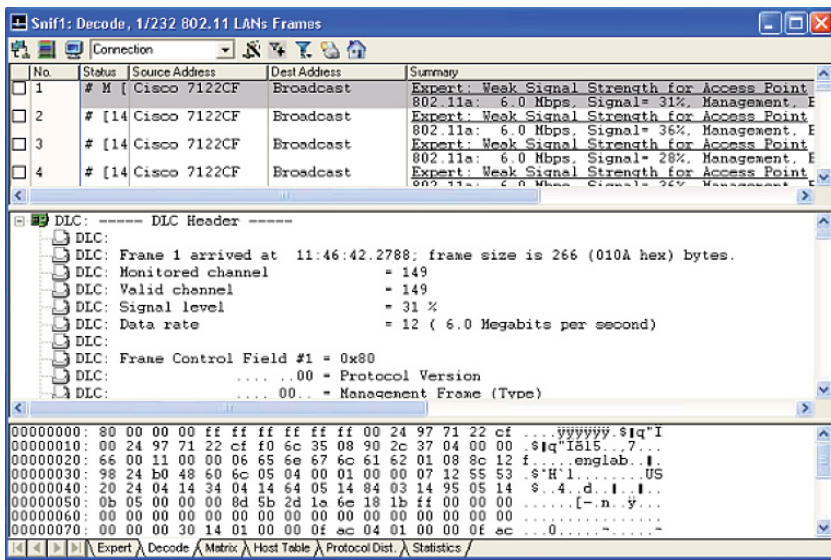
Figure 2: Sniffer Portable Professional decode view shows the results of a protocol analysis by displaying packets in three color-coded viewing panes: summary, detail, and hex codes.

Wireless Security Support

In addition to its existing support for WEP decryption, Sniffer Portable Professional can now decrypt WPA/WPA2 PSK (Personal) - encrypted data on 802.11 wireless networks. Users can specify shared passphrases for up to eight separate WPA/WPA2 PSK-encrypted SSIDs.

Rogue Access Point and Rogue Client Detection

Sniffer Portable Professional portable network analyzer automatically identifies and locates unauthorized devices operating in the Wi-Fi environment that may pose a risk to the overall security of the network. Users can establish an even higher level of organized security by designating a list of approved wireless devices monitoring for exposed wireless stations, ad-hoc devices, and other vulnerabilities.

Post capture, packets can be analyzed to determine if devices were being for denial of service attacks, flooding and other security policy violations.

Detailed Wireless Packet and Frame Analysis

Sniffer Portable Professional displays real-time packet flows for any Wi-Fi asset. Users can track data and management packets live, watch CRC errors, utilization, packet speed, media type and view a real-time decode page for detailed network analysis.

Specifications and System Requirements

Minimum Hardware Requirements:

- Intel or AMD processor running at 1.6 GHz single or higher or dual or more core running at 1.0 GHz or higher (IA-64 processor not supported)
- 512MB RAM or higher; 1GB recommend
- 200MB free disk space or more
- CD/DVD ROM drive
- VGA monitor with 1024x800 resolution and support for 256 color or updated VGA driver

Operating Systems Support:

- Microsoft® Windows® 7 (32-bit and 64-bit)
- Microsoft Windows Server® 2008 (32-bit or 64-bit)
- Microsoft Windows Vista® (32-bit or 64-bit)
- Microsoft Windows 2003 SP1 or later (32-bit or 64-bit)
- Microsoft Windows XP with SP2 or later (32-bit or 64-bit)
- Virtualized environments configured to emulate these operating systems, including VMware workstation/player, VMware® ESX/ESXi Server, and Microsoft Virtual-PC, and Hyper-V

Browser

- Microsoft Internet Explorer® 6.0 SP2, 7 or 8 browser

Network Interface Cards

- Ethernet 10/100/1000 cards with native driver provided by vendor
- Wireless 802.11a/b/g/n cards based on Atheros chipset with Sniffer enhanced driver (packaged with the software)

NOTE: NetScout recommends having two wireless cards on the system - one for sniffing and another for connectivity. If using the Location Tracking feature, connectivity through a second card (wired or wireless) is necessary.

NETSCOUT.

Americas East	Americas West	Asia Pacific	Europe
310 Littleton Road	178 E. Tasman Drive	17F/B	One Canada Square
Westford, MA 01886-4105	San Jose, CA 95134	No. 167 Tun Hwa N. Road	29th floor, Canary Wharf
Phone: 978-614-4000	Phone: 408-571-5000	Taipei 105, Taiwan	London E14 5DY, United Kingdom
Toll Free: 800-357-7666		Phone: +886 2 2717 1999	Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000